ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 32

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 11/03/2017

2. CONTRACT NO. *(If any)*: EP-W-17-020

3. ORDER NO.: 0003

4. REQUISITION/REFERENCE NO.: PR-OEI-18-00079

5. ISSUING OFFICE *(Address correspondence to)*:
HPOD
US Environmental Protection Agency
William Jefferson Clinton Building
1200 Pennsylvania Avenue, N. W.
Mail Code: 3803R
Washington DC 20460

6. SHIP TO:
a. NAME OF CONSIGNEE: Multiple Destinations
b. STREET ADDRESS:
c. CITY:
d. STATE:
e. ZIP CODE:

7. TO: [redacted]
a. NAME OF CONTRACTOR: INTERNATIONAL BUSINESS MACHINES CORPORATION
b. COMPANY NAME:
c. STREET ADDRESS: 6710 ROCKLEDGE DRIVE
d. CITY: BETHESDA
e. STATE: MD
f. ZIP CODE: 20817

f. SHIP VIA:

8. TYPE OF ORDER
☐ a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Schedule

10. REQUISITIONING OFFICE:

11. BUSINESS CLASSIFICATION *(Check appropriate box(es))*
☐ a. SMALL ☒ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT: Destination

13. PLACE OF
a. INSPECTION: Destination
b. ACCEPTANCE: Destination

14. GOVERNMENT B/L NO.:

15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*:

16. DISCOUNT TERMS:

17. SCHEDULE ***(See reverse for Rejections)***

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 835130485 The purpose of this Order is to procure the services of a contractor to provide support to the EPA Chief Information Security Officer (CISO), who is also the EPA Chief Privacy Officer, and responsible for Continued ...					

18. SHIPPING POINT:
19. GROSS SHIPPING WEIGHT:
20. INVOICE NO.:

17(h) TOTAL *(Cont. pages)*: $36,109,764.00

21. MAIL INVOICE TO:
a. NAME: RTP Finance Center
b. STREET ADDRESS (or P.O. Box): US Environmental Protection Agency
RTP-Finance Center (AA216-01)
109 TW Alexander Drive
www2.epa.gov/financial/contracts
c. CITY: Durham
d. STATE: NC
e. ZIP CODE: 27711

SEE BILLING INSTRUCTIONS ON REVERSE

17(i) GRAND TOTAL: $3,042,610.00

22. UNITED STATES OF AMERICA BY *(Signature)*: 11/03/2017 ELECTRONIC SIGNATURE

23. NAME *(Typed)*: Stefan Martiyan
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
11/03/2017	EP-W-17-020	0003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	developing and maintaining agency wide information security and privacy programs, developing and maintaining information security and privacy policies, procedures, and control techniques, training personnel with significant responsibilities, and assisting senior agency officials concerning information security and privacy responsibilities. TOCOR: Torina Anderson Max Expire Date: 10/31/2022 Admin Office: HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 Accounting Info: 18-WR-H1XXIT9-000HF8-2512-CISITSBZ-18H1CIS001-001 BFY: 18 Fund: WR Budget Org: H1XXIT9 Program (PRC): 000HF8 Budget (BOC): 2512 Job #: CISITSBZ DCN - Line ID: 18H1CIS001-001 Period of Performance: 11/01/2017 to 10/31/2018					
0001	Base Year Funding Award Type: Time-and-materials Delivery Location Code: HPOD Torina Anderson US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $3,042,610.00					
0002	Base Year Optional Tasks (Option Line Item) 364 Days After Award Delivery Location Code: HPOD HPOD US Environmental Protection Agency Continued ...				4,339,655.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $4,339,655.00

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
11/03/2017	EP-W-17-020	0003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $4,339,655.00					
0003	Option Year I Funding (Option Line Item) 10/31/2018 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $3,133,958.00				3,133,958.00	
0004	Option Year I Optional Tasks (Option Line Item) 10/31/2018 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $4,469,988.00				4,469,988.00	
0005	Option Year II Funding (Option Line Item) 10/31/2019 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $3,227,784.00				3,227,784.00	
0006	Option Year II Optional Tasks Continued ...				4,603,917.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $15,435,647.00

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
11/03/2017	EP-W-17-020	0003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	(Option Line Item) 10/31/2019 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $4,603,917.00					
0007	Option Year III Funding (Option Line Item) 10/31/2020 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $3,324,710.00				3,324,710.00	
0008	Option Year III Optional Tasks (Option Line Item) 10/31/2020 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $4,742,239.00				4,742,239.00	
0009	Option Year IV Funding (Option Line Item) 10/31/2021 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building Continued ...				3,407,329.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $11,474,278.00

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
11/03/2017	EP-W-17-020	0003

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $3,407,329.00					
0010	Option Year IV Optional Tasks (Option Line Item) 10/31/2021 Delivery Location Code: HPOD HPOD US Environmental Protection Agency William Jefferson Clinton Building 1200 Pennsylvania Avenue, N. W. Mail Code: 3803R Washington DC 20460 USA Amount: $4,860,184.00				4,860,184.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $4,860,184.00

Information Security and Privacy Services

1. PERFORMANCE WORK STATEMENT (PWS)

1.1. Background and Purpose

Information security technology will protect Agency data and make EPA WAN (Wide Area Network) resources available to more users and devices. With an information centric risk based approach, data can be categorized, segmented and controlled to offer additional services to internal and external customers.

This solution aligns with the Agency's strategic IT vision and the US Government's move to the Open Government Initiative (OGI). The solution offers the flexibility to embark on other strategic deployments such as cloud computing and mobile computing. The Tiered Network Solution should reduce the complexities of sharing data, yet be robust enough to protect and maintain the confidentiality, integrity, and availability (CIA) of the EPA Network information and resources through access control and monitoring methods.

1.2 Scope of Work

This Task Order provides support to the EPA Chief Information Security Officer (CISO), who is also the EPA Chief Privacy Officer, and responsible for developing and maintaining agency wide information security and privacy programs, developing and maintaining information security and privacy policies, procedures, and control techniques, training personnel with significant responsibilities, and assisting senior agency officials concerning information security and privacy responsibilities. EPA must adhere to legislative requirements and administrative mandates, and follow guidance and best practices recommended by the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and the Federal CIO and Privacy Councils.

This section states the performance-based objectives relating to this specific task. These objectives are related to and help satisfy overarching EPA objectives as well.

1) Project Management: All project activities are managed in accordance with the Project Management Institute's Body of Knowledge thus ensuring all tasks, activities, and deliverables are executed and delivered within required cost, quality, and schedule constraints.

2) Policy, Procedures, Standards, and Guidance: EPA information security and privacy documents provide the appropriate level of detail to reflect EPA adherence to active information security and privacy directives such as the Federal Information Security Modernization Act of 2014, the Privacy Act of 1974, National Institute of Standards and Technology publications, Office of Management and Budget memoranda and circulars, and EPA policy and procedures.

3) Compliance: Agency personnel provide information security and privacy in accordance with applicable directives for the information and information systems that support the operations and assets under their control.

4) Training: Personnel with significant information security and privacy responsibilities are adequately trained to perform their duties in EPA's environment. All users behave in a manner that indicates they are aware of their information security and privacy requirements and their associated responsibilities.

5) Oversight and Coordination: Personnel with significant information security and privacy responsibilities carry out these responsibilities adequately in accordance with applicable directives and have needed information to facilitate doing so.

6) Reporting: Information security data is gathered, validated, analyzed, and synthesized, resulting in accurate and complete responses to meet reporting requirements for standard and ad hoc reports and data calls. Resultant responses are properly prepared and forwarded to the appropriate EPA official with sufficient time for review, feedback, and correction prior to the data call response deadline.

7) Information Security and Privacy Programs Management: Processes are competently and effectively administered to help ensure the EPA Information Security and Privacy Programs excel in providing optimized risk based information protection.

8) Mission Assurance: Technical solutions and associated processes are thoroughly researched and expertly planned, implemented and integrated. The solutions and processes are complimentary and holistically developed to provide complimentary layered defenses while minimizing support and operations overhead.

1.3 TASKS

Task 1: Objective 1 – Task Management Reports:

a. Weekly Status Reports: The Contractor shall develop and provide weekly activity reports that include, but are not limited to, by Task, milestone progress to date, planned progress, deadlines, issues, and scope change request.
b. Monthly Project Status Report: The Contractor shall develop and provide monthly Earned Value Management (EVM) financial reports that provide EVM information by Task and for the overall TO.

    i. The report shall include financial and manpower information. The report shall include all cost elements and labor categories related to the TO and show hours expended and cost by labor category. Costs by element and hours and costs by labor category shall be provided for the reporting period and cumulative for the current period of performance.

Task 2: Objectives 2, 3 & 7 – EPA Information Security and Privacy Documents Maintenance:

a. The Contractor shall provide initial draft, updated, or new documents for review, changes, and comments. The Contractor shall provide subsequent drafts incorporating changes and comments provided during reviews for the following.

i. The Contractor shall review the EPA Information Security Strategic Plan (ISSP) and EPA Privacy Strategic Plan (PSP) annually and provide the CISO written recommendations for updating the plans. The Contractor shall update the plans according to CISO feedback.

ii. The Contractor shall develop an Information Security Program Plan (ISPP) to complement the ISSP. The ISPP shall build upon the ISSP providing particulars required by NIST publications for ISPP's not already provided in the ISSP. The Contractor shall review the ISPP annually and provide the CISO written recommendations for updating the ISPP. The Contractor shall coordinate and gather the requisite information to update the ISPP according to CISO feedback and update the ISPP annually.

iii. The Contractor shall develop a tactical plan annually that includes actions, milestones, deliverables and a deliverables schedule by Task to implement and support the implementation of the ISSP, ISPP, PSP and all Tasks and all exercised Optional Tasks. The Contractor shall update the tactical plan once per quarter based on CISO input.

iv. The Contractor shall coordinate with personnel to document EPA mission essential functions and related systems.

v. The Contractor shall coordinate with personnel to update the list of EPA mission essential functions and related systems developed in Task 2 item a. iv annually.

vi. The Contractor shall develop or support development of an EPA Critical Infrastructure Plan (CIP) incorporating results of Task 2 item a.iv.

vii. The Contractor shall review and update the EPA CIP incorporating results of Task 2 items a.iv and a.v.

viii. The Contractor shall obtain and review EPA Office of Inspector General (OIG), General Accounting Office (GAO), Department of Homeland Security (DHS) and other audit and review reports applicable to the EPA Information Security Program. The Contractor shall develop and provide corrective action plans (CAP), based on CISO input, for weaknesses identified in the reports for which the CISO has responsibility. Expect six corrective action plans per year.

ix. The Contractor shall execute the CAPs identified in Task 2 item a.viii.

x. The Contractor shall coordinate with the EPA Enterprise Architect and provide information to personnel to ensure the Information Security Enterprise Architecture (ISEA) is maintained current. The Contractor shall review and update the ISEA annually.

xi. The Contractor shall review minimum standard configurations to ensure they meet NIST, OMB, EPA and other information security and privacy directives' requirements. The Contractor shall provide written results of the standard configurations review providing correlating information on the particular portions of the configurations that do not meet requirements, which requirements have not been met, why they do not meet requirements, and recommendations on what is needed to meet requirements. Expect to review and provide comments and recommendations for 12 standard configuration documents per year.

xii. The Contractor shall review information security and privacy policies, procedures, guides, and standards developed in support of the EPA Information Security and Privacy Programs for adherence to and congruency with CISO, NIST, OMB, DHS and other information security and privacy directives. The Contractor shall provide comments and recommendations to correct or bring reviewed documents into

agreement. Expect to review and provide comments and recommendations for and update 12 such documents annually.

xiii. The Contractor shall obtain and review available control status information, e.g., control assessments, continuous monitoring results, vulnerability reports, audit reports etc., for indications of systemic issues and determine related controls, taking into account risk factors, that require enhanced focus to correct weaknesses and provide recommends to the CISO annually. The Contractor shall develop, maintain, and disseminate a list of "core" controls. Core controls are those identified that need enhanced focus to correct weaknesses. The Contractor shall update the list of core controls annually based upon the CISO's feedback on recommendations.

xiv. The Contractor shall review and update annually policy, procedures, standards, and guides for which the CISO is responsible. Expect 12 document reviews and updates annually.

xv. The Contractor shall review and update annually the risk management and continuous monitoring and Continuous Diagnostics and Mitigation (CDM) strategies.

Task 3: Objective 7 – Tactical Plan Execution:

a. The Contractor shall execute tactical plan tasks based on priorities, identified by the CISO, of the tactical plan developed and updated in Task 2.a.iii.
b. The Contractor shall develop process flows with narrative descriptions of how the processes work and how to execute them to include point of contact information for processes used to execute the tactical plan.
c. The Contractor shall update the process flows and narratives as the processes, points of contact and execution methods change.
d. The tactical plan shall be supported with status information on the execution efforts for the plan, e.g., accomplishments, challenges, critical milestones.
e. The tactical plan shall be updated to account for changing requirements and other factors that will affect plan and plan execution, e.g., new directives from OMB, available resources.
f. Changes and the reasons for the changes to the tactical plan shall be applied as appropriate to the strategic plan during the strategic plan update.

Task 4: Objectives 3 & 5 – POA&M Monitoring and Validation:

a. The Contractor shall coordinate and manage the POA&M Monitoring and Validation process, review submitted POA&Ms for accuracy and completeness, review submitted artifacts and determine whether they justify actions, e.g., closure, deletion, modification, or delay, provide monthly reports listing, grouped by office and system, POA&Ms reviewed with any associated deficiencies and correction recommendations, and review and update process documentation. Expect 125 systems with approximately 10 POA&Ms each.

b. The Contractor shall coordinate with personnel to obtain vulnerability, audit, security and privacy assessment and other reports and output that identify control weaknesses. The Contractor shall coordinate with report and output providers and system personnel

to verify accuracy and content and verify POA&Ms are documented accurately and according to requirements. Expect vulnerability reports every 72 hours, 10 OIG/GAO reports, and 125 security assessment reports annually.

Task 5: Objective 4 – Awareness Content Development and Process Coordination:

a. The Contractor shall annually review the annual user awareness content available on the EPA training site and provide recommendations to improve or update the content. The Contractor shall develop and provide content input to the awareness training tool maintenance group based on CISO feedback on Contractor provided recommendations.
b. The Contractor shall coordinate with personnel to develop an implementation schedule and execute the schedule.
c. The Contractor shall develop other awareness materials and content for dissemination on collaboration sites and other methods such as email, posters and flyers. Coordinate with personnel to, and disseminate the materials. Expect 15 development and dissemination actions annually.

Task 6: Objectives 6 – Maintain and update CISO systems' information in the EPA READ system:

a. The Contractor shall update systems annually when requested by the READ coordinator and provide completion notification to the READ coordinator, CISO and others as indicated in update instructions. Expect five CISO systems and one update per year.

Task 7: Objectives 3, 5, 6 & 7 – FISMA Reporting and Information and Artifact Repository / Governance, Risk and Compliance Tool Administration:

a. The Contractor shall provide user account maintenance and management and content maintenance and management. Content refers to the information the CISO is responsible for maintaining, and managing, e.g., controls delineated in NIST 800-53, EPA "core" controls, common and hybrid controls, listing reference documents, and systems identifiers and hierarchical structures. Expect to support 200 users and make 12 content updates annually.

b. The Contractor shall coordinate with the manufacturer and the infrastructure support service to ensure application updates, patches etc. are maintained up to date, that infrastructure support resources, e.g., memory, storage, and processing, are adequate to effectively support the user base, and that the configuration supports requirements to include templates, reports filtered on data points identified by the CISO, such as systems with personally identifiable information and mission essential systems, and integration with continuous monitoring tools and reporting. Expect six maintenance actions and one configuration review per year.

c. The Contractor shall coordinate with other system owners, contractors, and others to enable ingest and extraction of information and integration of the tool into other systems. Expect three such efforts annually.

Task 8: Objectives 5 – Develop and Maintain Infosec and Privacy Communications Sites:

a. The Contractor shall develop and maintain the content on an internally facing web site on existing EPA systems to disseminate information security related information to the EPA personnel. The site will include pertinent information such as information security awareness articles; information security program documents; and FAQ for policy and procedures interpretations. The Contractor shall update the design as needed and coordinate site implementation and maintenance. The site will target EPA users as well as specific groups such as ISO's. Expect minor updates monthly.

b. The Contractor shall develop and maintain the content on an internally facing collaboration sites on existing EPA systems to organize and support management of CISO office and Information Security and Privacy Program functions, disseminate information to EPA personnel and interact with the EPA information security population. The site will include pertinent information such as ISO meeting dates and times, agenda, and minutes; process flows; and data call information. The Contractor shall coordinate the design and implement the site. Expect updates monthly.

    a. The Contractor shall leverage collaboration tools' and other office automation tools' capabilities to automate CISO office and the Information Security and Privacy Program processes.

c. The Contractor shall manage access to collaboration sites as well as access and membership lists for email, active directory, and other mechanisms that facilitate coordination and information dissemination across the information security community.

Task 9: Objectives 6 & 7 – Information Security and Privacy Data Calls and Reporting Management:

a. The Contractor shall manage data calls to include coordination meetings and announcements, review, signoff, and explanatory meetings, status tracking and reporting, notifications and response generation. The Contractor shall gather, analyze, validate, and synthesize, information security and privacy data to meet reporting requirements for standard and ad hoc data calls. Resultant data call responses shall be prepared and forwarded to the CISO with sufficient time for review prior to the data call response deadline. Standard data calls are, for example, calls for quarterly and annual FISMA reports. Ad hoc calls are, for example, OIG, congressional inquiry, or GAO reports. Expect 10 data calls annually.

b. The Contractor shall coordinate with personnel to track annual awareness training completion to include obtaining verification of removing access to information and systems for users that do not complete. The Contractor shall provide three quarterly, two monthly, two weekly status reports and daily reports the week prior to the deadline to the CISO and a final report for the annual FISMA report. The Contractor shall ensure the reports are accurate and provide the required information.

c. The Contractor shall coordinate with personnel to obtain and validate information security and privacy control status information identified by the CISO and provide information security and privacy status reports. The reports shall include trends, narratives, and graphical representations that present the information in formats suitable for executives, information technology managers, information security officers and liaison privacy officers. Expect 23 program office and region specific and one enterprise level reports monthly.

Task 10: Objectives 3 & 7 – Interagency Agreements Management:

a. The Contractor shall coordinate with personnel and designated line of service providers to develop and maintain interagency agreements. Expect four interagency agreements.

b. The Contractor shall coordinate with personnel to process requests to obtain services from the line of service providers. The Contractor shall provide a schedule to process requests and process one request per interagency agreement per quarter. In addition to the quarterly requests, up to three ad hoc requests are expected annually.

c. The Contractor shall coordinate with the CISO, line of service providers, and others as necessary to develop statements of work and similar documents for each interagency agreement to obtain services from the providers. The Contractor shall update the documents annually to reinitiate the services.

d. The Contractor shall coordinate with CISO, line of service providers, and others as necessary to develop an annual assessment plan for all EPA systems. The Contractor shall coordinate execution of the plan with the respective services providers, systems owners, the CISO and others as necessary. The Contractor shall track and report progress of plan completion, provide recommendations to keep plan execution on schedule. Expect 125 system assessments per year.

Task 11: Objectives 3, 5, 6 & 7 – Audit and Review Process Management:

a. The Contractor shall coordinate with personnel to develop responses to the annual Federal Managers Financial Integrity Act (FMFIA) processes. The response encompasses reviewing and updating portions of related documents for which the CISO has direct responsibility or input into as related to the agency information security and privacy programs; reviewing the audit milestones provided by the Office of the Chief Financial Officer, comparing them to OIG audit reports, audit findings status reports, and providing written – in the format defined by the EPA Office of Chief Financial Officer – synopses, statuses, and updates for the milestones for which the CISO is responsible; and providing update input annually into appropriate CISO FMFIA milestones. The Contractor shall track the milestones and provide information and artifacts in accordance with the final milestones. The CISO is responsible for two to five milestones annually. Expect seven systems for review.

b. The Contractor shall coordinate with personnel to obtain OIG, GAO, DHS and other sources of audits and reviews reports and review for findings applicable to the

Information Security Program; identify and manage CISO related weakness findings in EPA's audit tracking tools and processes; provide input – documents, artifacts, answers – into the tools and processes and maintain and ensure tracking information is accurate, complete, and provided on-time; and develop, track, and execute CAPs for items for which the CISO is responsible. Expect six CISO related audits and reviews annually.

Task 12: Objectives 6 & 7 – Capital Planning and Investment Control Reporting:

a. The Contractor shall coordinate with personnel to review and update CPIC documents, gather data, and compile reports for the annual Exhibit 53 and related documents submission.

b. The Contractor shall gather and compile information for Exhibit 300/100 annual submission for CISO programs and systems. The Contractor shall update and maintain the documents in the agency's CPIC reporting tool. Expect five Exhibit 300/100's.

Task 13: Objectives 5 & 7 – Control Assessments Management:

a. The Contractor shall coordinate with personnel to schedule control assessments with the assessment service provider. The Contractor shall maintain, update, brief and disseminate the assessment schedule. The schedule shall project at least three years out and updated as schedule changes occur. Expect 125 systems on the schedule per year and seven updates annually.

Task 14: Objectives 5 & 7 – CISO and Information Security and Privacy Programs POA&M Management:

a. The Contractor shall coordinate with personnel to develop and maintain POA&Ms for system and program weaknesses for which the CISO is responsible. The CISO is responsible for five systems and EPA Information Security and Privacy Programs.

b. The Contractor shall execute and manage corrective actions in accordance with the POA&Ms.

c. The Contractor shall provide written notifications when milestones will be missed with the reason and recommendations to update the POA&M and meet new milestones.

Task 15: Objective 3 – Control Validation:

a. The Contractor shall conduct control testing to validate controls are implemented and operating as intended according to accreditation package artifacts. The Contractor shall conduct control testing on systems identified by the EPA CISO. The scope of the controls tested shall be limited to the controls identified by the EPA CISO, up to all controls identified as applicable in the NIST Special Publication 800-53 baseline

controls, FedRAMP and any additional controls implemented by system owners per assessment. The Contractor shall provide a report detailing the testing results to include all identified deficiencies and associated mitigation recommendations. Expect 11 systems annually.

Task 16: Objectives 4 & 7 – Role Based Training Program Development and Management:

a. The Contractor shall develop role-based training concentrations in the role-based training program for roles identified by the CISO. The training program will identify minimum requirements for each role based on the NIST NICE Framework where the minimum requirements will provide personnel with the knowledge and skills to perform their functions within EPA. Training available through EPA's training system and other no cost options shall be used to the maximum extent possible. The Contractor shall provide the CISO documentation detailing the program with recommendations and reasoning for program structure for review and approval. Upon approval, the Contractor shall provide the CISO a detailed implementation and management plan to include actions and milestones for review and approval. Expect eight roles in the program.

b. The Contractor shall coordinate with personnel to implement and manage the training program upon approval of the implementation and management plan.

c. The Contractor shall annually review curricula and coordinate with stakeholders to ensure training still provides desired goals. The Contractor shall identify available replacement training for any training identified as not meeting needs and coordinate to replace the outdated training with the new.

d. The Contractor shall coordinate with personnel to track annual role-based training completion to include obtaining verification of removing access to information and systems for users that do not complete annual training. The Contractor shall provide three quarterly, two monthly, and two weekly status reports to the CISO and a final report for the annual FISMA report. The Contractor shall ensure the reports are accurate and provide the required information.

Task 17: Objectives 4 & 7 – Credentialing Program Development and Management:

a. The Contractor shall develop role-based credentialing concentrations in the credentialing program for roles identified by the CISO. The concentrations will identify minimum credentials for each role and be based on the NIST NICE Framework. The Contractor shall provide an analysis of available third party professional credentials, where available for a particular role, e.g., CISSP, CAP, MCSE, for the experience, knowledge, and skill required to obtain each versus duties each role performs in EPA to determine which would be best indicators of needed competencies for EPA operations and which are most cost effective to obtain and maintain. The analysis shall include developing EPA credentials and obtaining and maintaining those versus available third party credentials. The evaluation shall include the use of training available through EPA's training system and other no cost options for achieving the third-party and EPA credentials. The analysis for the

credentialing program shall be coordinated with the development of the role-based training program so the combination results in the most effective programs for providing required knowledge and skills while being cost efficient. The Contractor shall provide the CISO documentation detailing the program with recommendations and reasoning for program structure for review and approval. Upon approval, the Contractor shall provide the CISO a detailed implementation and management plan to include actions and milestones for review and approval. Expect eight roles in the program.

b. The Contractor shall coordinate with personnel to implement and manage the credentialing program upon approval of the implementation and management plan.

c. The Contractor shall annually review credentials and coordinate with stakeholders to ensure they still provide desired goals. The Contractor shall identify available replacement credentials for any identified as not meeting needs and coordinate to replace the outdated with the new.

d. The Contractor shall coordinate with personnel to track credentialing completion. The Contractor shall provide three quarterly reports and one annual final report on status of progress and completion of personnel in the credentialing program. The Contractor shall ensure the reports are accurate and provide the required information.

Task 18: Objective 3 – Information Security and Privacy Information Maintenance and Authorization Package Reviews:

a. The Contractor shall coordinate with personnel to input, review, update and maintain accurately and completely, system and program information security and privacy information in the FISMA Reporting and Information and Artifact Repository / Governance, Risk and Compliance Tool for each system, control set, e.g., common controls and program – agency or organization level. This includes but is not limited to systems' interdependence/interfaces, control inheritances, and system type, e.g., cloud, PII/SPII, contractor.

b. The Contractor shall coordinate with personnel to review submitted authorization packages for quality, completeness, accuracy and expectation of meeting adequate security and privacy in accordance with an approved review checklist. The Contractor shall work with personnel to ensure significant deficiencies are corrected or documented in a POA&M prior to submitting authorization packages are submitted to the CISO for review. The Contractor shall provide the review results by submitting the completed checklist, a summary report that lists each discovered discrepancy with an associated recommended action for each package, memos and other documents according to the process.

c. The Contractor can choose to use a Contractor supplied review checklist or one supplied by the EPA CISO. The Contractor supplied review checklist shall be approved by the EPA SAIO before it can be used. The Contractor shall maintain the review checklist, whether Contractor or EPA CISO supplied, current as directives and

processes change. Any changes to the review checklist that impact the substance of the review parameters shall be approved by the EPA CISO before use.

d. The Contractor shall coordinate with personnel to process and submit process documents and coordinate review meetings according to the review process. Expect to review and coordinate 125 systems annually.

Task 19: Objective 4 – FISMA Reporting and Information and Artifact Repository / Governance, Risk and Compliance Tool Training:

a. The Contractor shall provide scheduled and ad hoc training for tool users on how to use the tool and how to correlate the tool and tool flow processes into related agency processes. Expect 12 scheduled training sessions per year. Each scheduled training session will be approximately 2 hours long. Expect two ad hoc training sessions per month. Each ad hoc training session will be approximately ½ hour long.

b. The Contractor shall provide and update when needed training materials, e.g., power point slides, written step-by-step guides, and templates, with instructions for data input and update within the tool for particular process steps to facilitate the training as well as use of the tool.

c. The Contractor shall coordinate with personnel to accurately input and maintain information in the tool. Information shall be maintained in a consistent manner, e.g., consistent control descriptions from system to system and consistent control inheritance from common control providers to dependent systems. Expect 125 systems.

Task 20: Objective 7 – Transition-In

a. The Contractor shall execute its Transition-In Plan no later than (NLT) five workdays after Project Start (PS). During the transition-in, the Contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed 30 calendar days after PS). The Contractor shall provide a Transition-in Plan at Kickoff Meeting based on the Contractor's proposed plan.

Task 21: Objective 7 – Transition-Out

a. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming Contractor/Government personnel at the expiration of the TO. The Contractor shall provide a Transition-Out Plan NLT 120 calendar days prior to expiration of the TO. The Contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

   i. Project management processes.
   ii. Points of contact (POCs).
   iii. Technical and project management documentation.
   iv. Status of ongoing technical initiatives.

v. Appropriate contractor–to-contractor/government coordination to ensure a seamless transition.
vi. Transition of Key Personnel.
vii. Schedules and milestones.
viii. Actions required of the Government.

The Contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings. The Contractor shall execute transition-out activities IAW the Government-approved Transition-Out Plan. The Contractor shall implement the TO Transition-Out Plan NLT 30 calendar days prior to expiration of the TO.

Task 22: Objectives 6, 7 and 8 Developing and Maintaining Systems and Program Security and Privacy Documentation

a. The Contractor shall coordinate with the CISO, the OEI Information Security Officer (ISO), Information Management Officer (IMO), Senior Information Official (SIO), and others as necessary to ensure FISMA requirements are met, e.g., develop and maintain information security documentation, ensure control assessments are accomplished, maintain and manage POA&Ms, weaknesses are mitigated, and an authorization to operate is maintained current for CISO systems. Expect five systems to review and update authorization packages annually, annual control assessment reports, POA&Ms annually per system, and reauthorization triennially. After ongoing authorizations are establish in EPA, the Contractor will provide and update information necessary to maintain ongoing authorizations.

b. The Contractor shall coordinate with the CISO, the OEI IMO, the OEI Capital Planning and Investment Control (CPIC) group, and others as necessary to maintain accurately and current the Information Security and Privacy Program and CISO system CPIC documentation. Expect updates biannually.

Optional Tasks:

The following optional tasks may only be exercised and ordered by the Contracting Officer via a modification to the task order. Al optional tasks will be identified as optional tasks in the task order award.

Optional Task 1: Objective 7 Determining Need for Specially Configured Devices for International Travelers:

a. The Contractor shall coordinate with EPA personnel to determine the need for specially configured devices for international travelers. The CISO will provide the guidance necessary to make the determination from the CISO's perspective. The Contractor shall coordinate with the EPA intelligence support office to obtain their determination and

inform requestors whether specially configured devices are needed. The Contractor can expect six requests weekly. This work requires Secret clearance.

Optional Task 2: Objective 8 – Security Engineering

a. The Contractor shall coordinate and consult with personnel to:
    a. Evaluate functional requirements and translate functional requirements into technical solutions.
    b. Design, develop, test, and evaluate information system security throughout the systems development lifecycle.
    c. Develop system architects.
    d. Prepare use cases.
    e. Analyze design constraints, trade-offs, and detailed system and security designs.
    f. Develop and test application of security policies on information technology.
    g. Design and develop secure interface specifications.
    h. Design control standards for hardware, operating systems, and software applications.
    i. Develop, disseminate, and brief detailed security design documentation and supporting documentation.
b. The Contractor shall coordinate and consult with personnel to:
    a. Conduct software and systems engineering and research in order to develop new capabilities, ensuring cybersecurity is fully integrated.
    b. Conduct comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.
    c. Provide input to cyber capabilities strategies.
    d. Identify functional and security related features.
    e. Research and evaluate all available technologies and standards.
    f. Research current technology.
    g. Develop, disseminate, and brief detailed documentation and supporting documentation.
c. The Contractor shall coordinate and consult with personnel to:
    a. Develop and maintain business, systems, and information processes to support enterprise mission needs; develops information technology rules and requirements that describe baseline and target architectures.
    b. Design enterprise and systems security throughout the development life cycle; translate technology and environmental conditions, e.g., law and regulation, into security designs and processes.
    c. Collaborate with system developers.
    d. Document design specifications.
    e. Evaluate current or emerging technologies.
    f. Develop, disseminate, and brief detailed documentation and supporting documentation.

d. The Contractor can expect six (6) efforts per year.

Optional Task 3: Objectives 8 & 9 – Security Operations

a. The Contractor shall coordinate and consult with personnel to:
    a. Coordinate and execute penetration and social engineering testing, red team evaluations, vulnerability assessments and other similar measurements of control effectiveness and defense capabilities.
        1. Identify deviations from EPA policy, procedures, standards, guides and other information security directives, and OMB, DHS, NIST, DISA and other federal information security directives and references. Where such directives or references do not exist, identify deviations from industry recognized best practices.
        2. Measure effectiveness of defense-in-depth architecture against known threats.
        3. Analyze results of tests and exercises to determine effectiveness of security controls including security training.
        4. Provide lessons learned and reports to include recommendations for improvement.
        5. Develop and process for approval rules of behavior for each engagement.
        6. The Contractor can expect six engagements per year.

    b. Monitor systems for events using a variety of cyber defense tools, e.g., IDS alerts, firewalls, and network traffic logs, and analyze events for and alert and follow up on suspicious activity.
        1. Lead and conduct incident response processes - determine and execute actions to mitigate and minimize the impact of threats and malicious and other activity that is contrary to information security directives.
        2. Collect information and conduct forensics work on systems and devices to determine root causes and support response and mitigation actions.
        3. Track and report events and incidents.

    c. Assist with baseline configuration management.

    d. Periodically delineate and provide assessments of threats to EPA and EPA systems and information.

    e. Develop, disseminate, and brief detailed documentation and supporting documentation.

Optional Task 4: Objective 7 – Immediate Office Operations

a. The Contractor shall coordinate and consult with personnel to:
    a. Develop and implement office standards and procedures.
    b. Coordinate office training activities.
    c. Develop, document and manage the Cybersecurity and Privacy service catalog and associated operational level agreements and service level agreements.
    d. Coordinate the CISO's and DCISO's travel, meetings and calendars. To include compilation of materials, note taking, agenda development and information dissemination.
    e. Manage logistics and facilities requests.
    f. Develop and disseminate crisis and routine communications.

g. Develop and disseminate "Marketing" Plan for customers.
h. Monitor for data calls, gather pertinent information, develop responses and track data call requests and responses.
i. Support budget development and management and track expenditures and deviations from budget plans.
j. Provide graphics designer support with:
    1. Timely creation and completion of daily intelligence products that are delivered to officials at the highest levels of Government. Design and layout of interactive briefing products, guides, manuals, programs, flat panel displays, seals, boards and other collateral materials for events, projects and conferences.
    2. Design and layout graphic images that enhance the presentation of information in support of OISP primarily through print services, web, collaboration sites and CD-ROM.
    3. Provide graphic support leveraging the tools and software provided by the CISO or by the Contractor with approval from the CISO to securely deliver and present, organize and market information.
    4. Interpret requirements, identify the most efficient presentation of intelligence products and develop preliminary concepts that communicate intelligence information consistent with EPA style guidelines.

Optional Task 5: Objectives 5, 6 & 7 – Continuous Monitoring and Continuous Diagnostics and Mitigation Operations

a. The Contractor shall conduct the operation of the continuous monitoring (CM) and continuous diagnostics and mitigation (CDM) solutions. While EPA designated system administrators and cybersecurity personnel will have access to the CM/CDM tools and sensors, including their product consoles, the Contractor shall be responsible for the operation of the overall solutions.

Optional Task 6: Objectives 6, 7 & 8 – Tier Two and Tier Three Support for Continuous Monitoring and Continuous Diagnostics and Mitigation Operations

a. The Contractor shall coordinate its Tier Two and Three support with the Tier One provider, EPA help desk and the Department of Homeland Security's (DHS) CDM Dashboard Provider's Help Desk. The Contractor shall provide Tier Two and Tier Three support for the CM/CDM solutions, except Tier Three support for the CDM Dashboard, which will be provided by the DHS CDM Dashboard Provider. The Contractor shall provide support during the normal workweek (Monday through Friday) and shall provide coverage from 0800 through 1800 hours Eastern Time (ET).
    i. Tier One support will include problem resolution using standard methodologies and basic troubleshooting techniques including EPA-raised issues, incident and request management, access and inventory management, change and configuration management, security, and patch management consistent with EPA's policies and procedures.
    ii. The Contractor shall provide Tier Two support. Tier Two support shall include more in-depth troubleshooting and shall require specialized knowledge of CM/CDM solutions and EPA CDM Dashboards for remediation.

iii. The Contractor shall provide Tier Three support for the CM/CDM solutions. Tier Three support shall include advanced engineering support to include coordination and resolution with solution's original equipment manufacturers (OEMs). All calls determined by Tier Two to be related to the CDM Dashboard and not resolved through Tier Two shall be forwarded to the DHS CDM Dashboard Provider for Tier Three support.

b. The Contractor shall establish a procedure for recording and a ticket tracking mechanism for all operational support requests. The Contractor shall use the EPA supplied ticket tracking tool or one provided by the Contractor upon approval by the CISO. The Contractor shall report on a monthly basis the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved in the weekly status report – Task 1. The Contractor shall, at a minimum, provide the following support:
   i. Provide initial problem resolution where possible.
   ii. Generate, monitor, and track incidents through resolution.
   iii. Provide software support.
   iv. Maintain frequently asked questions (FAQs) and their resolutions.
   v. Obtain customer feedback and conduct surveys.

Optional Task 7: Objectives 6, 7 & 8 – Tier One Support for Continuous Monitoring and Continuous Diagnostics and Mitigation Operations

c. The Contractor shall coordinate its Tier One support with the Tier Two and Three providers and the EPA help desk. The Contractor shall provide support during the normal workweek (Monday through Friday) and shall provide coverage from 0800 through 1800 hours Eastern Time (ET).
   i. Tier One support will include problem resolution using standard methodologies and basic troubleshooting techniques including EPA-raised issues, incident and request management, access and inventory management, change and configuration management, security, and patch management consistent with EPA's policies and procedures.

d. The Contractor shall establish a procedure for recording and a ticket tracking mechanism for all operational support requests. The Contractor shall use the EPA supplied ticket tracking tool or one provided by the Contractor upon approval by the CISO. The Contractor shall report on a monthly basis the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved in the weekly status report – Task 1. The Contractor shall, at a minimum, provide the following support:
   vi. Provide initial problem resolution where possible.
   vii. Generate, monitor, and track incidents through resolution.
   viii. Provide software support.
   ix. Maintain frequently asked questions (FAQs) and their resolutions.
   x. Obtain customer feedback and conduct surveys.

Optional Task 8: Objectives 7 & 8 – Plan for Production Operations

a. The Contractor shall develop a Plan for Production Operations. The Plan for Production Operations (PPO) shall describe how the Contractor will operate the CM/CDM solutions to meet CM/CDM objectives outlined EPA CM/CDM strategic plans and CONOPS. The Plan for Production Operations shall include, at a minimum, the following:
   i. Testing Methodology.

ii. Description of configuration management methodology for the tools and sensors of the CM/CDM solutions. Plan shall include incorporation of CM/CDM services on all assets of EPA's infrastructure, including applications, servers, and desktops.
iii. Ensure that the CM/CDM solutions collect data on at least 95 percent of devices in each set of two successive scans within the 72-hour window.

b. O&M Methodology
   i. Identify requirements needed to operate the CM/CDM solutions through the entire life of the TO.
   ii. Describe detailed activities that support the EPA CM/CDM strategic plans and CONOPS.
   iii. Determine data relevant for inclusion in the weekly status report.
   iv. Describe Operational Analysis for Post-Implementation Reviews.
   v. Description of configuration management methodology for the tools and sensors of the CM/CDM solutions.
   vi. Description of Change Management methodology for the tools and sensors of the CM/CDM solutions.

Optional Task 9: Objectives 7 & 8 – Production Operations

a. The Contractor shall operate the CM/CDM solutions consistent with the Plan for Production Operations. The Contractor shall monitor the CM/CDM solutions for system performance and functionality and elevate any issues. The Contractor shall incorporate the CM/CDM solutions into the respective EPAs' continuous monitoring activities. The CM/CDM solutions shall operate consistent with EPA system security requirements.
b. The Contractor shall perform problem management in coordination with EPA personnel for the CM/CDM solutions by identifying problems and performing resolution, to include notifying OEM vendors of application issues. The Contractor shall initiate formal requests for any EPA infrastructure modifications and follow change control procedures.
c. The Contractor shall submit reports of technical metrics on the operation of CM/CDM solutions as defined in the PPO in the weekly status report.

Optional Task 10: Objectives 7 & 8 - Maintain Interoperability between CM/CDM solutions and EPA Legacy Applications and Data

a. The Contractor shall maintain interoperability between the CM/CDM solutions and other EPA legacy applications for the purpose of sharing data.
b. Examples of legacy applications include, but are not limited to, the following:
   i. Discovery tools.
   ii. Network asset systems (e.g., Active Directory and other Lightweight Directory Access Protocol (LDAP)-like systems).
   iii. Property management systems.
   iv. Configuration management systems.
   v. Vulnerability management systems.
   vi. Open Checklist Interactive Language (OCIL) questionnaire systems.
b. The Contractor shall periodically perform the appropriate data exchanges between EPA legacy applications and the CM/CDM solutions as to ensure the CM/CDM solutions uses the most current data as defined by the EPA policy. The Contractor shall update the data exchange mechanism in response to changes in either the EPA legacy applications or the CM/CDM solutions.

Optional Task 11: Objectives 7 & 8 – Operate Data Feeds to/from Installed CDM Dashboards

a. The Contractor shall operate and maintain the CDM Dashboard data feeds, utilizing the Security Content Automation Protocol (SCAP)-compliant Asset Summary Reporting Format (ASR), between the following:
    i. The CM/CDM solutions integration point and EPA CDM Dashboards.
    ii. The EPA CDM Dashboards to the CDM Federal Dashboard - summary level data only.

Optional Task 12: Objectives 7 & 8 – Provide Governance Support

a. The Contractor shall use CDM governance guidelines that are being developed by the DHS CDM Program Office to provide governance support to EPA.
b. The Contractor shall use its knowledge of the CM/CDM solutions and the DHS CDM Program Office-provided CDM program guidance to assist EPA to develop or improve EPA-specific CDM governance structures and policies.
c. The Contractor shall deliver a Draft and Final CDM Governance Support Plan. The CDM Governance Support Plan shall include:
    i. Assessment of existing cybersecurity governance environment (including processes, organizational structures, and relationships) at EPA.
    ii. Recommendations/best practices to establish, modify or improve, and manage EPA's CDM Program, following DHS guidance. Recommendations/best practices shall include at a minimum the following:
    1. Processes for developing or improving and managing EPA-specific CDM governance structures.
    2. Integration of DHS CDM governance best practices into EPA CM/CDM or broader information security governance structures and policies.
    3. Process for developing and/or updating the EPA's CM strategy required by OMB M-14-03.
    4. Strategy for establishing/improving and managing EPA-specific CM/CDM working groups and encouraging EPA participation in the DHS CDM working groups.
    5. The Contractor shall provide a recommendation outlining the structure and level of effort of the ongoing support of CDM governance (primarily consisting of CDM working group(s)).
    6. The Contractor shall conduct initial working group(s) for presenting CDM governance to the D/A CDM stakeholders.

Optional Task 13: Objectives 7 & 8 – Support Independent Verification and Validation (IV&V) and System Authorization

a. The Contractor shall provide the project management, engineering, data, and documentation necessary to conduct testing, support independent verification and validation (IV&V) efforts, and support system authorization.
b. The Contractor shall provide a Security Model with Documentation to update the Authorization Package, as identified below.
c. The Contractor shall perform security authorization activities on the EPAs' CM/CDM solutions to include the following:
    i. Provide EPA with all required documentation to support EPA's security authorization (in ongoing authorization format), to include inputs to relevant

portions of the System Security Plan (e.g., system description, system architecture, security controls). This shall include periodic updates to accommodate EPA's authorization refresh and re-authorization events.

ii. Provide technical support to the EPA's security authorization process related to the CM/CDM solutions:
    1. Security Test and Evaluation/Security Assessment activities.
    2. Remediation of findings or creation of Plans of Action and Milestones (POA&Ms) as appropriate.
    3. Incorporation of CM/CDM solutions into the EPA's continuous monitoring activities.

Optional Task 14: Objectives 2, 3, 4, 5, 6, 7, & 8 – Information Security Office and Information System Security Officer Support

a. The Contractor shall coordinate with personnel to provide ISO support for 50 systems by:
    a. Supporting the AA or RA by managing activities identified under the EPA Information Security Program and ensuring protection measures are compliant with FISMA and related information security directives for the information, information systems, and services for their office or region to include but not limited to:
    b. Coordinating with the CISO in developing, documenting, implementing, and maintaining an office or region and Agency-wide information security programs to protect EPA information and information systems.
    c. Coordinating with the CISO in responding to information security data calls, audit requests, and reporting.
    d. Implementing policies, procedures, and control techniques identified in the Agency information security program.
    e. Providing guidance on their roles and responsibilities and Agency information security program requirements to ISSOs, system administrators, and others with significant security responsibilities.
    f. Tracking and ensuring all EPA information and information system users within their organizations successfully complete information security awareness training prior to initial access to EPA systems and information and at least annually thereafter to maintain access. Ensuring access is removed for users who do not successfully complete awareness training.
    g. Tracking and ensuring all employees within their organizations designated as having significant information security responsibilities complete role based information security training and credentialing, as defined under the EPA Information Security Program.
    h. Making determination for acceptability of training to meet role based training, education, and credentialing requirements in accordance with information security training and education program requirements. Referring to CISO for final determination as necessary.
    i. Enforcing and ensuring the NROB, and additional system specific rules of behavior where applicable, are reviewed and signed or acknowledged electronically or manually prior to being granted access to EPA information and information systems and annually thereafter to maintain access. Ensuring access is removed for users who do not do so.

j. Supporting the SIO in ensuring effective processes and procedures and other directives are established as necessary to implement the policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and enforced for their office or region by taking actions to include but not limited to:
k. Ensuring systems have an authorization to operate or authorization to test from the appropriate SIO prior to operational use or testing in an operational environment.
l. Reviewing periodically the Agency information security system inventory tool and ensuring systems are reported accurately and completely.
m. Reviewing periodically the Agency information security information repository and ensuring all system information security information, such as plans of actions and milestones, system security plans, and security assessment reports, are entered and maintained accurately and up to date.
n. Coordinating with the CIO, Risk Executive, Risk Executive Group, CISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.
o. Monitoring POA&Ms to ensure weakness remediation and mitigation are managed and actions are documented properly.
p. Coordinating and liaising with local, other EPA, and external personnel for system and information security management, operations and control monitoring, audits, assessments, incident response, and law enforcement investigations.
q. Coordinating with CSIRC as a first responder for incidents affecting the assigned organization's information, systems or personnel.
r. Providing expert advice in developing and updating enterprise and local information security documents to include policy, procedures, standards and guides.
s. Coordinating with and supporting the IMO and AODR in implementing EPA Information Security Program requirements.
t. Supporting system owners, information owners, and service managers in developing and maintaining system information security documentation, obtaining and maintaining authorization to operate or test, and ensuring systems are configured, continuously monitored, and maintained to adequately protect supported information within acceptable risks by taking actions to include but not limited to:
u. Providing expert advice in:
    i. developing and updating mandatory configurations for information technology products and solutions used by EPA;
    ii. determining local controls to ensure compatibility and interoperability with enterprise tools and controls;
    iii. implementing, operating, and maintaining enterprise tools and controls;
    iv. ensuring information and systems are properly categorized;
    v. defining, developing, documenting, implementing, assessing, and monitoring all controls to include common and hybrid controls;
    vi. conducting impact analyses for proposed or actual changes to systems or their operational environments; and
    vii. Developing and implementing system decommissioning and information disposal strategies.

b. The Contractor shall provide ISSO support for 50 systems by:

    a. Supporting the SIO, SO, SM, IO and ISO in managing and implementing the activities, processes, policies, procedures, control techniques, and other countermeasures identified under the EPA Information Security Program and ensuring protection measures are compliant with FISMA and related information security directives for the information, information system, and service assigned by taking actions to include but not limited to:
        i. Ensuring the day-to-day security operations of an information system, including verifying that security controls, technical and otherwise, are functioning as intended.
        ii. Developing and maintaining in coordination with system administrators and others involved with implementing and maintaining controls, the system security plan, including appendices, the contingency plan and other documents required for information systems' authorization packages.
        iii. Ensuring systems have an authorization to operate or authorization to test from the appropriate SIO prior to operational use or testing in an operational environment.
        iv. Reporting systems in the Agency information security system inventory tool and maintaining current and accurate information.
        v. Entering into the Agency information security information repository and all system information security information, such as plans of actions and milestones, system security plans, and security assessment reports, and maintaining current and accurate information.
        vi. Coordinating with the CIO, Risk Executive, Risk Executive Group, CISO and others involved with securing Agency information and systems to ensure risks are managed to an acceptable level.
        vii. Responding to information security data calls, audit requests, and reporting.
        viii. Providing expert advice in:
            1. developing and updating mandatory configurations for information technology products and solutions used by EPA;
            2. determining local controls to ensure compatibility and interoperability with enterprise tools and controls;
            3. implementing, operating, and maintaining enterprise tools and controls; and
            4. ensuring information and systems are properly categorized.
    b. Serving as a principal advisor on all matters, technical and otherwise, involving the security of information, information system, or services assigned.
    c. Implementing policies, procedures, and control techniques identified in the Agency information security program.

Optional Task 15: Objective 7 – Federal Wide Coordinating Continuity of Operations (COOP) Exercise:

a. The Contractor shall coordinate with personnel, review and provide input into the annual federal wide COOP exercise documents, and provide synopsis and status reports to the CISO on exercise planning and execution. Expect 10 exercise documents.

b. The Contractor shall attend planning meetings providing input and recording CISO actions items and provide meeting notes and synopsis to include a brief to inform other EPA personnel of the exercise, actions, and requirements to the CISO. Expect six meetings for the annual exercise.

Optional Task 16: Objective 7 – Performance Plan Measures and Job Descriptions Development

a. The Contractor shall coordinate with personnel to develop and update as needed standard performance plan measures and job descriptions for roles identified in the information security and privacy role based training programs.

Optional Task 17: Objective 7 – Performance Measurement Management:

a. The Contractor shall develop, document, and implement and update as needed a performance measurement program for the information security and privacy programs and OISP functions.
b. The Contractor shall measure and document program performance according to the program requirements.
c. The Contractor shall analyze performance measurement results quarterly and provide program status reports, develop and provide recommendations to address any weaknesses identified, including metrics, and develop trends.

Optional Task 18: Objectives 4 & 7 – Annual Information Security Conference Support:

a. The Contractor shall coordinate with personnel to develop agenda topics and conference schedules, arrange guest speakers' participation, and develop supporting documents.
b. The Contractor shall provide on-site conference support at two locations to register users, coordinate testing, coordinate system and site configuration, and track attendance.
c. The Contractor shall provide training materials and training sessions for EPA tools and program processes and directives, policy and procedures during the conference. Expect four training sessions per conference.

Optional Task 19: Objective 2 – Insider Threat Program

a. The Contractor shall coordinate with personnel to develop and update program documents. Expect to review three documents annually.
b. The Contractor shall monitor for, evaluate and notify of indicators of malicious and suspicious insider activities.
c. The Contractor shall take actions and coordinate with personnel according to EPA procedures, federal directives and best practices to mitigate malicious and suspicious insider activities.
d. The Contractor shall coordinate with personnel and conduct analyses of malicious and suspicious insider activities to include determining root causes to develop after action reports and lessons learned that include recommendations to mitigate weaknesses identified.

Optional Task 20: Objectives 3 & 6 – Risk Assessments

a. The Contractor shall coordinate with personnel to conduct assessments of risk. Risk assessment reports shall include recommendations for risk mitigation for the various risk mitigation options. Assessments include the evaluation of mobile apps using an EPA supplied tool. Expect to conduct 50 risk assessments annually.

Optional Task 21: Objectives 3 & 6 – Security Impact Analyses

a. The Contractor shall coordinate with personnel to analyze changes to information systems to determine potential security impacts. The security impact analysis report shall include recommendations on making the changes. Expect to conduct six security impact analyses annually.

Optional Task 22: Objectives 5, 6 & 7 – Security Control Assessments

a. The Contractor shall coordinate with personnel to conduct security control assessments in accordance with NIST publications and EPA policy and procedures. The security assessment report shall include recommendations for risk mitigation for the various risk mitigation options. Expect to conduct 60 security control assessments annually.

Optional Task 23: Objectives 7 & 8 – Project Management

a. The Contractor shall conduct project management activities. This includes the management or coordination, oversight and quality assurance of all activities performed by personnel to develop project artifacts, coordinate personnel, conduct research, manage meetings, track status and budgets, identify and track risks, develop and implement technical solutions and associated processes to successfully meet project objectives.
b. The Contractor shall use industry-best standards and proven methodologies that assure all project activities are identified, documented, and tracked so that projects can continuously be evaluated and monitored for timely and quality service. The Contractor shall notify the CISO of any technical, financial, personnel, or general managerial problems encountered throughout the life of each project. Expect to support up to five projects annually.
    a. The Contractor must develop project management capabilities into a framework that is based on industry best practices defined by PMI PMBOK and aligned to ITIL standards.
    b. The Contractor's framework should consist of the following but are not limited to: a detailed roadmap, processes and procedures, templates, critical decision points, and gate reviews.
        i. The roadmap must align the entire project lifecycle with requirements set forth in the scope statements.
        ii. The individual schedules must be rolled up into an integrated master schedule.
    c. The Contractor must assist in defining scope, schedule and costs, which could include but is not limited to risk assessments, customer evaluations and feedback.
        i. The Contractor will review performance metrics and perform trending analysis to identify variances between planned and actual performance.

ii. The Contractor will update processes, systems and partner relationships to ensure quality project management and implementation support.

1.4 Reporting Requirements and Deliverables

The contractor shall prepare a Quality Assurance Project Plan for this task order. See clause 2.1 under the "Inspection and Acceptance" section below.

For most deliverables, the EPA TOCOR will assign tentative due dates and instructions when work is routed to the Contractor. If within three business days, the contractor expresses no concern regarding the due date; the date shall be deemed settled by tacit agreement.

The contractor shall provide a monthly technical and financial progress report as per the contract, see attached template. The report shall be submitted on or before the 15th of each month (following the completion of the first reporting period), with a copy provided (preferably by email) to the EPA Contract level COR and TOCOR. Among other data required, the report shall list each review action completed (finished and delivered) during the reporting period, along with its data package bar code, number of studies, percentage complete and labor hours (if required by task). These stipulations will not reduce any of the contractual monthly reporting obligations. Content and format of the monthly technical and financial progress report must be intelligible and must be sufficient to support the agency's review of invoicing, budget status, and technical progress. Any new reporting needs found may be requested by technical direction to the degree permissible under the task order.

SCHEDULE OF DELIVERABLES:

Deliverable	Schedule	Format/Distribution
Quality Assurance Project Plan http://www.epa.gov/quality/epa-quality-management-tools-projects	Within 14 calendar days after task Order is awarded	Email to Contract-level COR and respective TOCOR
Monthly Progress Report	15th of each month (following completion of 1st reporting period)	Email a copy to the CO, Contract level COR and TOCOR
Data Review Action	Provided through technical direction in current EPA MS Word version, via email, etc., Contractor has three business days to respond to the TOCOR any concerns, and renegotiation regarding the due date	MS Word (2013) or current EPA compatible software format, using acceptable electronic media or via email per action to the TOCOR
Transition In Plan	Five (5) business days from the start of the Order.	Provide to Contract Level COR at Kick Off Meeting

Transition Out Plan	120 days before Order expires	Provide to Contact Level COR

1.5 Acceptable Quality Level for Tasks

See Attachment: Quality Assurance Surveillance Plan

1.6 Method of surveillance

Reports prepared by the contractor undergo a secondary review process in OPP. Each report has a designated EPA reviewer. The EPA reviewer conducts a detailed review of the contractor's summary of relevant data and examines the conclusions drawn by the contractor in accordance with the criteria described in the task Order. Once the EPA reviewer has finalized the data evaluation in the form of an Agency review, the report may be used officially. The EPA reviewer will complete an EPA Reviewer's Assessment Form that notes discrepancies, omissions, inaccuracies and/or inappropriate data evaluations ("errors"). The TOCOR or Contract Level COR will calculate, quarterly, the average number of reports containing substantive technical, guideline, or format errors. The CORs will compare agency due dates or approved revised due dates to completed date of reports, quarterly and calculate the percentage of late reports. See attachment J.5 of this RFTOP.

1.7 Period of Performance

The period of performance of this task order is:

Base: November 1, 2017 – October 31, 2018
Option 1: November 1, 2018 – October 31, 2019
Option 2: November 1, 2019 – October 31, 2020
Option 3: November 1, 2020 – October 31, 2021
Option 4: November 1, 2021 – October 31, 2022

1.8 Task Order Type (Firm Fixed Price or Time & Materials):

This Order will be a Time and Materials Order.

2. INSPECTION AND ACCEPTANCE

2.1 Quality Assurance Project Plan

The Contractor shall submit the following quality system documentation to the CO at the time frames identified below:

	Documentation	Specifications	Due
X	Quality Assurance Project Plan for the Task Order	EPA Requirements for Quality Assurance Project Plans (QA/R-5) [dated	14 Calendar Days after

		03/20/11]	Award

This documentation can be found on the following EPA website – https://www.epa.gov/quality/epa-qar-5-epa-requirements-quality-assurance-project-plans

This documentation will be prepared in accordance with the specifications identified above or equivalent specifications defined by EPA.

The Government will review and return the quality documentation, with comments, and indicating approval or disapproval. If necessary, the contractor shall revise the documentation to address all comments and shall submit the revised documentation to the government for approval.

The Contractor shall not commence work involving environmental data generation or use until the Government has approved the quality documentation.

3. TASK ORDER ADMINISTRATION DATA

3.1 Contract Administration Representatives

Contracting Officer: Sheila Dolan, dolan.sheila@epa.gov

Contract Specialist: John Moua, moua.john@epa.gov

Contract Level Contracting Officer's Representative: Kim Farmer, farmer.kim@epa.gov

Task Order Contracting Officer's Representative: Torina Anderson, anderson.torina@epa.gov

3.2 INVOICING

Invoices shall be submitted in accordance with the contract under which this task order is awarded through FedConnect to the CO, CS, and TOCOR. Invoices shall be submitted electronically to: US EPA FINANCE OFFICE AT DDC-KINVOICES@EPA.GOV

For format and guidance refer to: http://www2.epa.gov/financial/contracts#Contract_invoices
The customer service contact information for the finance office is contractpaymentinfo@epa.gov and 919-541-1148.

4. TASK ORDER CLAUSES

4.1 FAR 52.217-7 Option for Increased Quantity -- Separately Priced Line Item (Mar 1989)

The Government may require support for Optional Tasks 1-23, identified in the Performance Work Statement as optional services at the labor rates proposed in the offeror's pricing proposal. The Contracting Officer may exercise the option by written notice to the Contractor within *14 calendar days of task order*

award. Delivery of optional services shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of Clause)

4.2 FAR 52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

4.3 FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this order by written notice to the Contractor within 5 calendar days before the expiration of this order; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the order expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this order, the extended order shall be considered to include this option clause.

(c) The total duration of this order, including the exercise of any options under this clause, shall not exceed 60 months.

(End of clause)